



In the Claims

The status of claims in the case is as follows:

1 1. [Currently amended] A method of operating a virtual
2 private network (VPN) based on IP Sec that integrates
3 network address translation (NAT) with IP Sec processing,
4 comprising the steps executed at one end of a VPN connection
5 of:

6 configuring a VPN NAT IP address pool on a VPN gateway
7 machine at said one end of a VPN connection employing
8 only IP address data available at said VPN gateway
9 machine;

10 configuring at said one end of said VPN connection a
11 VPN connection to utilize said VPN NAT IP address pool;

12 obtaining at said one end of said VPN connection a
13 specific IP address from said VPN NAT IP address pool,
14 and allocating said specific IP address for said VPN
15 connection;

16 starting said VPN connection;

17 loading to an operating system kernel at said one end
18 of said VPN connection the security associations and
19 connection filters for said VPN connection;

20 processing at said one end of said VPN connection a IP
21 datagram for said VPN connection; and

22 applying VPN NAT at one end of said VPN connection to
23 said IP datagram with source and destination port
24 values after the application of VPN NAT being the same
25 as before application of VPN NAT.

1 2. [Original] The method of claim 1, wherein said VPN
2 connection is configured for outbound processing, and said
3 applying step comprises outbound source IP Nating.

1 3. [Original] The method of claim 1, wherein said VPN
2 connection is configured for some combination of inbound
3 processing, and said applying step selectively comprises
4 inbound source IP NATing or inbound destination IP NATing.

1 4. [Original] The method of claim 1, further for

2 integration of NAT with IP Sec for manually-keyed IP Sec
3 connections, comprising the further step of manually
4 configuring connection keys.

1 5. [Original] The method of claim 1, further for
2 integrating NAT with IP sec for dynamically-keyed (e.g. IKE)
3 IP Sec connections, comprising the further step of:
4 configuring the VPN connections to obtain their keys
5 automatically.

1 6. [Original] The method of claim 1, further for
2 integrating NAT with IP Sec Security Associations,
3 negotiated dynamically by IKE, wherein said starting step
4 further comprises creating a message for IKE containing said
5 IP address from said NAT pool; and further comprising the
6 step of operating IKE to obtain dynamically negotiated keys.

1 7. [Original] The method of claim 6, further comprising
2 the step of combining the dynamically obtained keys with
3 said NAT pool IP address and wherein said loading step loads
4 the result as security associations into said operating
5 system kernel.

1 8. [Currently amended] A computer implemented method for
2 allowing the definition and configuration of NAT directly
3 with definition and configuration of IPsec-based VPN
4 connections and VPN policy, comprising the steps executed by
5 a digital processor at one end of a VPN connection of:

6 configuring at one end of said VPN connection the
7 requirement for VPN NAT by a yes/no decision in a
8 policy database for each of the three types of VPN NAT,
9 said three types being VPN NAT type a outbound source
10 IP NAT, VPN NAT type c inbound source IP NAT, and VPN
11 NAT type d inbound destination IP NAT; [[and]]

12 configuring at said one end of said VPN connection on a
13 VPN gateway machine at said one end of a VPN connection
14 employing only IP address data available at said VPN
15 gateway machine a remote IP address pool or a server IP
16 address pool selectively responsive to said yes/no
17 decision for each said VPN NAT type; and

18 upon subsequent start of said VPN connection,
19 processing inbound and outbound packets at said one end
20 of said VPN connection responsive to configuration of
21 said VPN NAT in said policy database and configuration

22 of said remote IP address pool.

1 9. [Previously presented] The computer implemented method
2 of claim 8, further comprising the step of configuring a
3 unique said remote IP address pool for each remote address
4 to which a VPN connection will be required, whereby said
5 remote IP address pool is keyed by a remote ID.

1 10. [Previously presented] The computer implemented method
2 of claim 8, further comprising the step of configuring said
3 server IP address pool once for a system being configured.

1 11. [Currently amended] A computer implemented method of
2 providing customer tracking of VPN NAT activities as they
3 occur in an operating system kernel, comprising the steps
4 executed at one end of a VPN connection of:

5 responsive to VPN connection configuration, generating
6 journal records as a log entry in a file system of an
7 operating system at said one end of said VPN
8 connection;

9 updating at said one end of said VPN connection said
10 journal records with new records for each datagram

1 12. [Currently amended] A computer implemented method of
2 allowing a VPN NAT address pool to be associated with a
3 gateway, thereby allowing server load- balancing, comprising
4 the steps executed by a digital processor at one end of a
5 VPN connection of:

6 configuring at said one end of said VPN connection a
7 server VPN NAT IP address pool for a system being
8 configured;

9 storing at said one end of said VPN connection specific
10 IP addresses that are globally routable in said server
11 VPN NAT IP address pool;

12 configuring at said one end of said VPN connection a
13 VPN connection to utilize said server VPN NAT IP
14 address pool; and

15 managing at said one end of said VPN connection total
16 volume of concurrent VPN connections responsive to the

17 number of addresses in said server VPN NAT IP address
18 pool with source and destination port values before and
19 after application of VPN NAT being the same.

1 13. [Currently amended] A method of controlling the total
2 number of VPN connections for a system based on availability
3 of VPN NAT addresses, comprising the steps executed at one
4 end of a VPN connection of:

5 configuring on a VPN gateway machine at said one end of
6 said VPN connection employing only IP address data
7 available at said VPN gateway machine the totality of
8 remote IP address pools with a common set of IP
9 addresses, said addresses being configured as a range,
10 as a list of single addresses, or any combination of
11 multiple ranges and single addresses; and

12 limiting at said one end of said VPN connection the
13 successful start of concurrently active VPN connections
14 responsive to the number of said IP addresses
15 configured across the totality of said remote address
16 pools.

1 14. [Currently amended] A method of performing virtual

2 private network (VPN) network address translation on
3 selected ICMP datagrams, comprising the steps executed at
4 one end of a VPN connection of:

5 combining at said one end of said VPN connection IP
6 Security & VPN NAT by detecting selected types of ICMP
7 type packets; and

8 responsive to said selected types, performing at said
9 one end of said VPN connection network address
10 translation functions on the entire datagram including
11 ICMP data.

1 15. [Currently amended] A method of performing virtual
2 private network (VPN) network address translation on
3 selected FTP datagrams, comprising the steps executed at one
4 end of a VPN connection of:

5 combining at said one end of said VPN connection IP
6 Security & NAT by detecting the occurrence of FTP PORT
7 or PASV FTP commands; and

8 responsive to said command, performing at said one end
9 of said VPN connection network address translation on

10 the FTP data and the header.

1 16. [Currently amended] A computer system for operating a
2 virtual private network (VPN) based on IP Sec that
3 integrates network address translation (NAT) with IP Sec
4 processing executed by a digital processor at one end of a
5 VPN connection, comprising:

6 means for configuring on a VPN gateway machine at said
7 one end of a VPN connection a VPN NAT IP address pool
8 employing only IP address data available at said VPN
9 gateway machine;

10 means for configuring at said one end of said VPN
11 connection a VPN connection to utilize said VPN NAT IP
12 address pool;

13 means for obtaining at said one end of said VPN
14 connection a specific IP address from said VPN NAT IP
15 address pool, and allocating said specific IP address
16 for said VPN connection;

17 means for starting said VPN connection at said one end
18 of said VPN connection;

19 means for loading at said one end of said VPN
20 connection to an operating system kernel the security
21 associations and connection filters for said VPN
22 connection;

23 means for processing at said one end of said VPN
24 connection a IP datagram for said VPN connection; and

25 means for applying at said one end of said VPN
26 connection VPN NAT to said IP datagram with source and
27 destination port values after application of VPN NAT
28 being the same as before application of VPN NAT.

1 17. [Currently amended] A system for definition and
2 configuration of NAT directly with definition and
3 configuration of VPN connections and VPN policy executed by
4 a digital processor at one end of a VPN connection,
5 comprising:

6 a policy database for configuring at said one end of
7 said VPN connection the requirement for VPN NAT by a
8 yes/no decision for each of the three types of VPN NAT,
9 said three types being VPN NAT type a outbound source
10 IP NAT, VPN NAT type c inbound source IP NAT, and VPN

11 NAT type d inbound destination IP NAT; and

12 a remote IP address pool or a server IP address pool at
13 said one end of said VPN connection selectively
14 configured on a VPN gateway machine at said one end of
15 a VPN connection responsive to said yes/no decision for
16 each said VPN NAT type employing only IP address data
17 available at said VPN gateway machine.

1 18. [Currently amended] A system implemented at one end of
2 a VPN connection for allowing a VPN NAT address pool to be
3 associated with a gateway, thereby allowing server
4 load-balancing, comprising:

5 a server VPN NAT IP address pool on a VPN gateway
6 machine at said one end of a VPN connection configured
7 for a given system being configured for containing
8 multiple address addresses configured as a range, as a
9 list of single addresses, or any combination of
10 multiple ranges and single addresses employing only IP
11 address data available at said VPN gateway machine;

12 said server VPN NAT IP address pool storing specific IP
13 addresses that are globally routable;

14 a VPN connection at said one end of said VPN connection
15 configured to utilize said server VPN NAT IP address
16 pool; and

17 a connection controller for managing at said one end of
18 said VPN connection total volume of concurrent VPN
19 connections responsive to the number of addresses in
20 said server VPN NAT IP address pool with source and
21 destination port values after application of VPN NAT
22 being the same as before application of VPN NAT.

1 19. [Currently amended] A program storage device readable
2 by a machine, tangibly embodying a program of instructions
3 executable by a machine to perform method steps executed at
4 one end of a VPN connection for operating a virtual private
5 network (VPN) based on IP Sec that integrates network
6 address translation (NAT) with IP Sec processing, said
7 method steps comprising:

8 configuring on a VPN gateway machine at said one end of
9 a VPN connection a NAT IP address pool employing only
10 IP address data available at said VPN gateway machine;

11 configuring at said one end of said VPN connection a

13 obtaining a specific IP address from said VPN NAT IP
14 address pool, and allocating at said one end of said
15 VPN connection said specific IP address for said VPN
16 connection;

```
17     starting said VPN connection at said one end of said  
18     VPN connection;
```

19 loading to an operating system kernel at said one end
20 of said VPN connection the security associations and
21 connection filters for said VPN connection;

22 processing at said one end of said VPN connection a IP
23 dataagram for said VPN connection; and

24 applying at said one end of said VPN connection VPN NAT
25 to said IP datagram with source and destination port
26 values after application of VPN NAT being the same as
27 before application of VPN NAT.

1 20. [Currently amended] An article of manufacture
2 comprising:

3 a computer useable medium having computer readable
4 program code means embodied therein for operating a
5 virtual private network (VPN) based on IP Sec that
6 integrates network address translation (NAT) with IP
7 Sec processing executed at one end of a VPN connection,
8 the computer readable program means in said article of
9 manufacture comprising:

10 computer readable program code means for causing a
11 computer to effect configuring a VPN NAT IP address
12 pool on a VPN gateway machine at said one end of a VPN
13 connection employing only IP address data available at
14 said VPN gateway machine;

15 computer readable program code means for causing a
16 computer to effect configuring at said one end of said
17 VPN connection a VPN connection to utilize said VPN NAT
18 IP address pool;

19 computer readable program code means for causing a
20 computer to effect obtaining at said one end of said
21 VPN connection a specific IP address from said VPN NAT
22 IP address pool, and allocating said specific IP
23 address for said VPN connection;

24 computer readable program code means for causing a
25 computer to effect starting at said one end of said VPN
26 connection said VPN connection;

27 computer readable program code means for causing a
28 computer to effect loading at said one end of said VPN
29 connection to an operating system kernel the security
30 associations and connection filters for said VPN
31 connection;

32 computer readable program code means for causing a
33 computer to effect processing at said one end of said
34 VPN connection a IP datagram for said VPN connection;
35 and

36 computer readable program code means for causing a
37 computer to effect applying at said one end of said VPN
38 connection VPN NAT to said IP datagram with source and
39 destination port values after the application of VPN
40 NAT being the same as before application of VPN NAT.

1 21. [Currently amended] A computer implemented method for
2 providing IP security in a virtual private network using
3 network address translation (NAT), comprising the steps

4 executed by a digital processor at one end of a VPN
5 connection of:

6 dynamically generating at said one end of said VPN
7 connection NAT rules and associating them selectively
8 with manual [[or]] and dynamically generated (IKE)
9 Security Associations; thereafter

10 beginning at said one end of said VPN connection IP
11 security that uses the Security Associations; and then

12 as IP Sec is performed on outbound and inbound
13 datagrams, selectively performing at said one end of
14 said VPN connection one or more of VPN NAT type a
15 outbound source IP NAT, VPN NAT type c inbound source
16 IP NAT, and VPN NAT type d inbound destination IP NAT.

1 22. [Currently amended] The method of claim 1, said VPN
2 NAT IP address pool containing multiple addresses configured
3 as a range, as a list of single address, or any combination
4 of multiple ranges and single addresses.